Entrust/PKI and You

We Bring Trust to e-Business™

Printed in Canada.

Release 6.0.

Contents

Entrust/PKI and You

This document provides an overview of Entrust/PKI. You should read this document if you want an introduction to public-key infrastructures and a quick overview of Entrust Technologies' products and services. This document is suitable for new Entrust/PKI administrators, or anyone within your organization who wants to learn more about Entrust/PKI and its operation.

Topics in this document include

If you require more detailed information on public-key infrastructures and Entrust Technologies' products and services after reading this document, please refer to our Web site, located at

www.entrust.com

What can Entrust/PKI do for me?

Entrust Technologies provides security solutions for e-business. To do this, Entrust software allows you to place trust in all forms of electronic transactions. Trust is gained through user authentication, digital signatures and the protection of confidential information.

While all organizations have a need for security, not all organizations' security needs are the same. Possible security needs include

- keeping personal documents secret and secure
- keeping e-mail secret and secure
- verifying the origin of a document or e-mail
- establishing the time at which a document or e-mail was created or sent
- deleting files securely
- ensuring that a wide variety of software and hardware components (such as Web browsers and wireless devices) can transmit information securely and confidentially
- ensuring that all of the above requirements can be carried out simply and transparently

In addition to providing these services for their users, an organization's planners and administrators may have other security requirements such as

- comprehensively managing security policies
- supporting roaming users
- allowing user-based self-registration and administration
- enabling secure communications and transactions over intranets, extranets, and the Internet
- providing controlled resource access to employees, customers, or partners
- providing secure access to virtual private networks (VPNs)
- providing secure access to enterprise resource planning (ERP) software
- providing secure communications over wireless devices
- enforcing security through cryptographic hardware devices
- developing and customizing security solutions through software toolkits

The solution for all of these security needs? Use a *PKI*.

What's a PKI?

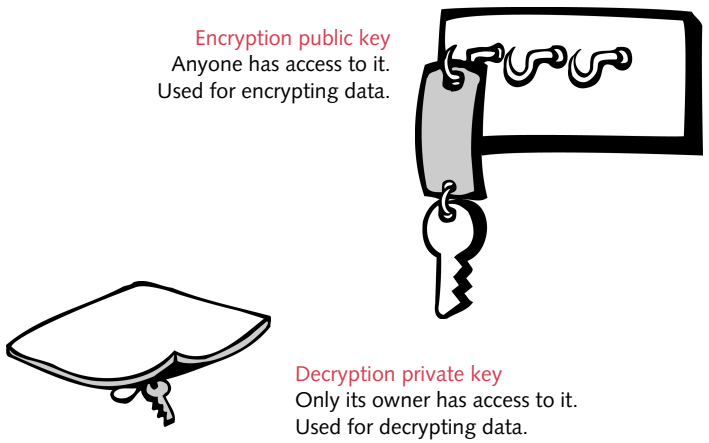
PKI stands for *public-key infrastructure*. Entrust Technologies enables secure e-business by using a PKI as the basis for all its security solutions. To understand how a PKI provides security, you must first understand three underlying concepts: *security through cryptography*, *certificates*, and the *Certification Authority*.

Security through cryptography

To keep data secure, and to provide a user with a digital signature, each user has a number of different keys. The keys that keep data secure are the *encryption key pair*, used in conjunction with *symmetric keys.* The keys that provide a digital signature are known as the *signing key pair*.

Data security using the encryption key pair and symmetric keys

The encryption key pair, used in conjunction with symmetric keys, keeps data secure. The encryption key pair consists of a public key (used only for "locking"—that is, *encrypting*—data, known as the *encryption public key*) and a private key (used only for "unlocking"—that is, *decrypting*—data, known as the *decryption private key*). Encrypting and decrypting data through the use of a public-private encryption key pair is known as *asymmetric cryptography,* or, as it is more popularly known, *public-key cryptography*.



The additional keys used for data security are known as *symmetric keys*. A symmetric key is like a physical key people use in their daily lives, in which the key is used to both lock and unlock items. Symmetric keys, then, are used for both encrypting and decrypting data. This process is known as *symmetric cryptography*. The primary benefit of symmetric encryption is speed. Because of

this, symmetric algorithms are especially suited to encrypting and decrypting large amounts of data.

Symmetric key

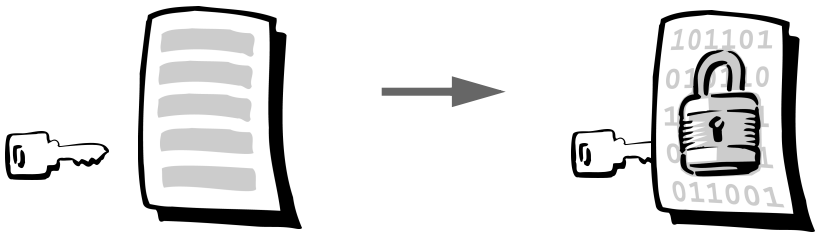
Used for both encrypting and decrypting data.

The process of using both symmetric-key and public-key cryptography to secure data involves the following steps:

1 The sender "locks" the data (that is, *encrypts* it) with a one-time symmetric key, generated randomly for this step.

Normal data
In its normal state the data is readable.

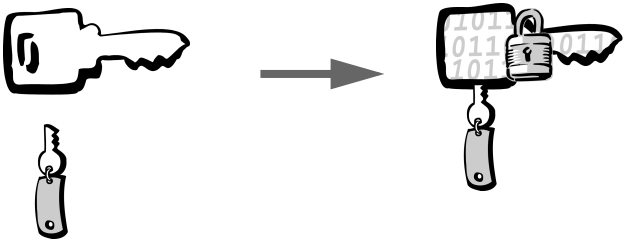
Encrypted data
In its encrypted state the data is unreadable.



2 The sender then encrypts the symmetric key with the *recipient's* encryption public key.

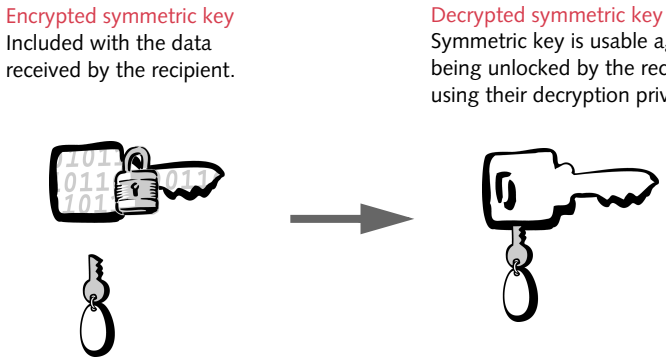
Symmetric key
In its unencrypted state the symmetric key can be used to decrypt any data it has previously encrypted.

Encrypted symmetric key
In its encrypted state the symmetric key is unusable.



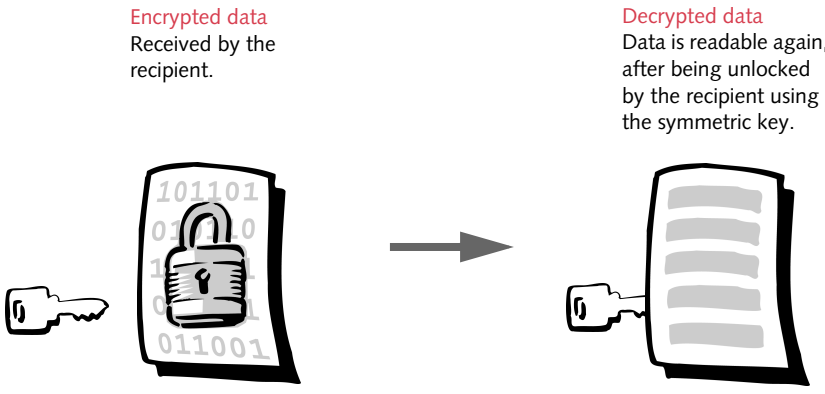
Next, the sender forwards both the encrypted data and the encrypted symmetric key to its intended recipient.

3 After receiving the encrypted data and the encrypted symmetric key, the recipient first "unlocks" the symmetric key (that is, *decrypts* it) with their decryption private key.



Remember: since the sender locked the symmetric key using the *recipient's* encryption public key, only the recipient's decryption private key is capable of unlocking it.

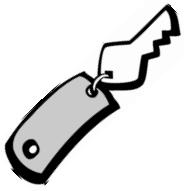
4 With the symmetric key usable again, the recipient uses it to decrypt the data.



Digital signatures using the digital signature key pair

The digital signature key pair provides a user with the means of generating a digital signature. A digital signature provides a guarantee to a recipient that signed data came from the person who signed it, and that it was not altered since it was signed. The digital signature key pair is composed of a signing key (known as the *signing private key*) and a verification key (known as the *verification public key*).

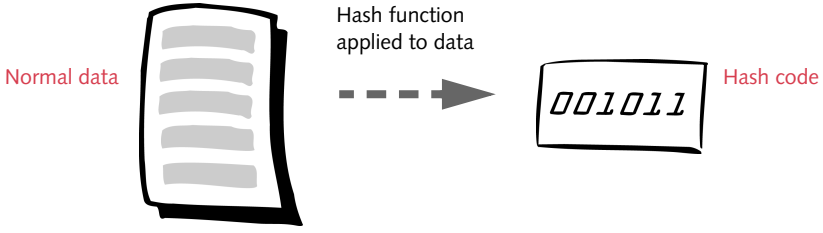
Signing private key
Privately held by its owner to sign data. No other users have access to it.



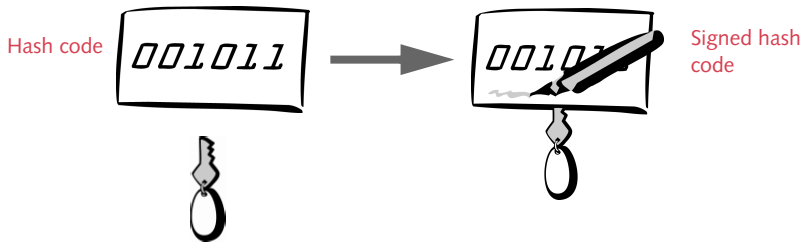
Verification public key
A non-secret key used to verify a signature. It proves that the signature was signed by its matching signing private key.

To affix a digital signature, a sender follows these steps:

1 The sender starts the process by taking a mathematical summary (called a *hash code*) of the data. This hash code is a uniquely identifying digital fingerprint of the data. If even a single bit of the data changes, the hash code will change.



2 Next, the sender *encrypts* the hash code with their signing private key.

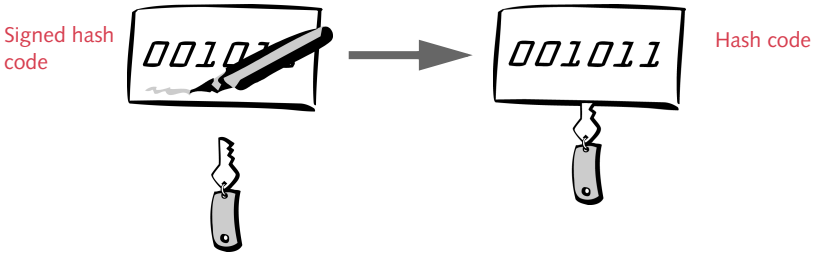


The sender then forwards the data and the encrypted hash code (that is, the signature) to the intended recipient.

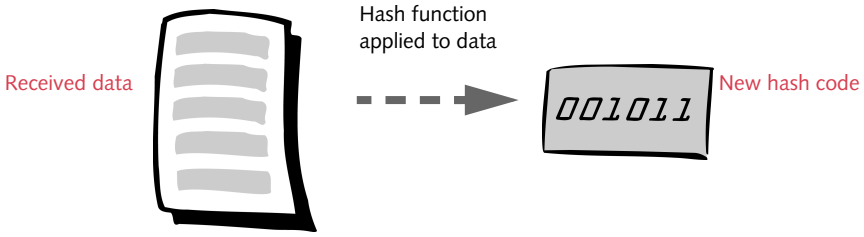
How can the encrypted hash code be considered a signature? The encrypted hash code is an item that only the sender, using their signing private key, could have produced.

The next series of steps describes verification of the signature and confirmation that the data has not been altered since it was signed.

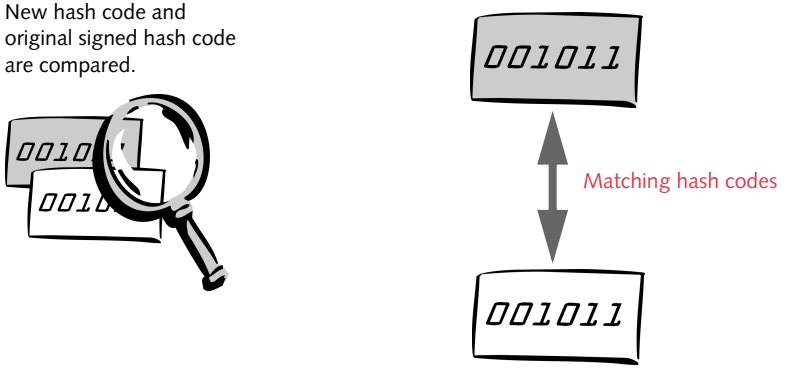
1 Upon receipt of the data and the encrypted hash code, the recipient can verify that the hash code was encrypted by the sender by decrypting the hash code using the *sender's* verification public key.



2 The recipient, having possession of what presumably is the original data, uses the data to generate a new hash code.



3 The new hash code and the decrypted hash code are compared. If the hash codes match, the recipient has verified that the data has not been altered.



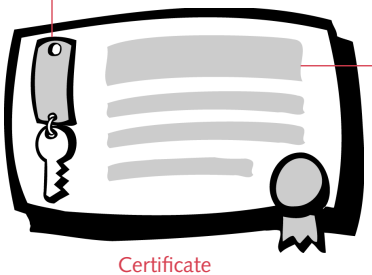
How do matching hash codes indicate that the data was not altered since the signature was created? Because the hash function that produced the hash codes is extremely sensitive to changes in data. If the data had been altered in any way, the new hash code it produced would not have been identical to the original hash code. Matching hash codes ensure the data is in the same state that it was in when it produced the original hash code—thus proving that no altering of data has taken place.

Remember: a digital signature guards data against modification, but it does not prevent unauthorized eyes from viewing the data. To protect data against unauthorized access, you must also encrypt the data.

Certificates

Using public and private keys to encrypt and sign data raises an important security-related question: how can you be sure the public key you are using belongs to the right person?

The solution: associate the public key and its user with a *certificate*.



Certificate

A certificate is an object that contains (among other items)

- information, in an industry-standard format, detailing the person's identity
- a public key, associated exclusively with the person

Certification Authority

A certificate associates a public key with an individual user.

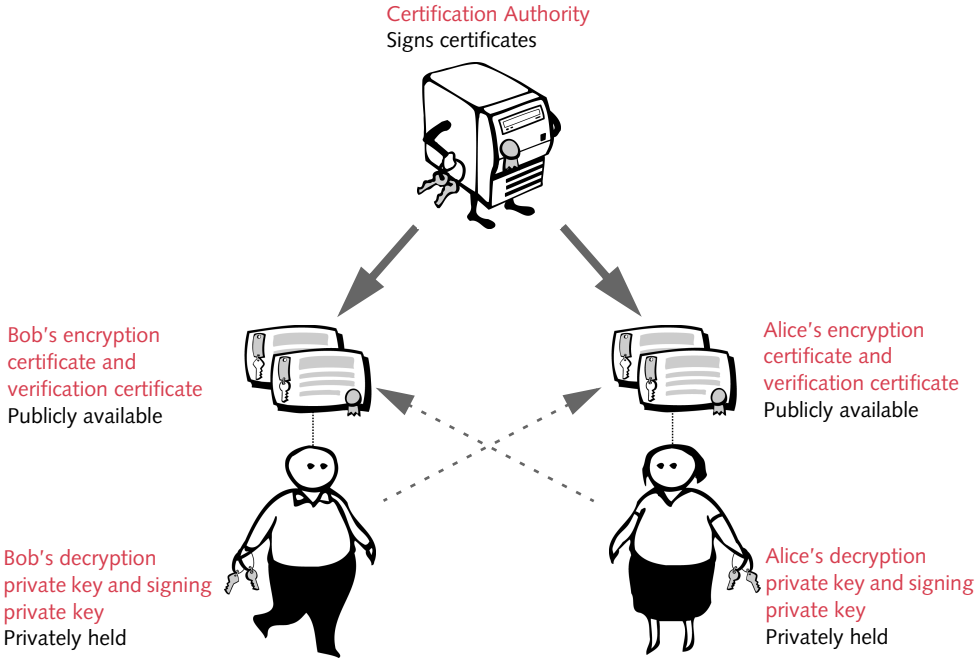
But how do you know that the information in the certificate is valid? How do you know that the correct public key has been associated with its rightful user?

The solution: have the information in all certificates guaranteed by a *Certification Authority.*

Certification Authority

A Certification Authority is a trusted entity whose central responsibility is certifying the authenticity of users. In essence, the function of a Certification Authority is analogous to that of the passport issuing office in the Government. A passport is a citizen's secure document (a "paper identity"), issued by an appropriate authority, certifying that the citizen is who he or she claims to be. Any other country trusting the authority of that country's Government passport office will trust the citizen's passport. This is an example of *third-party trust*.

Similar to a passport, a user's certificate is issued and signed by a Certification Authority and acts as proof that the correct public key is associated with the user. Therefore, through third-party trust, anyone trusting the Certification Authority can also trust the user's key.



If Bob or Alice trust the Certification Authority, they can be sure that the certificates signed by it are associated with their rightful owner. With this trust established, encryption can take place, with the sender knowing that only the intended recipient will be able to decrypt the data, and verification can take place, with the recipient knowing that only the signer could have signed the data.

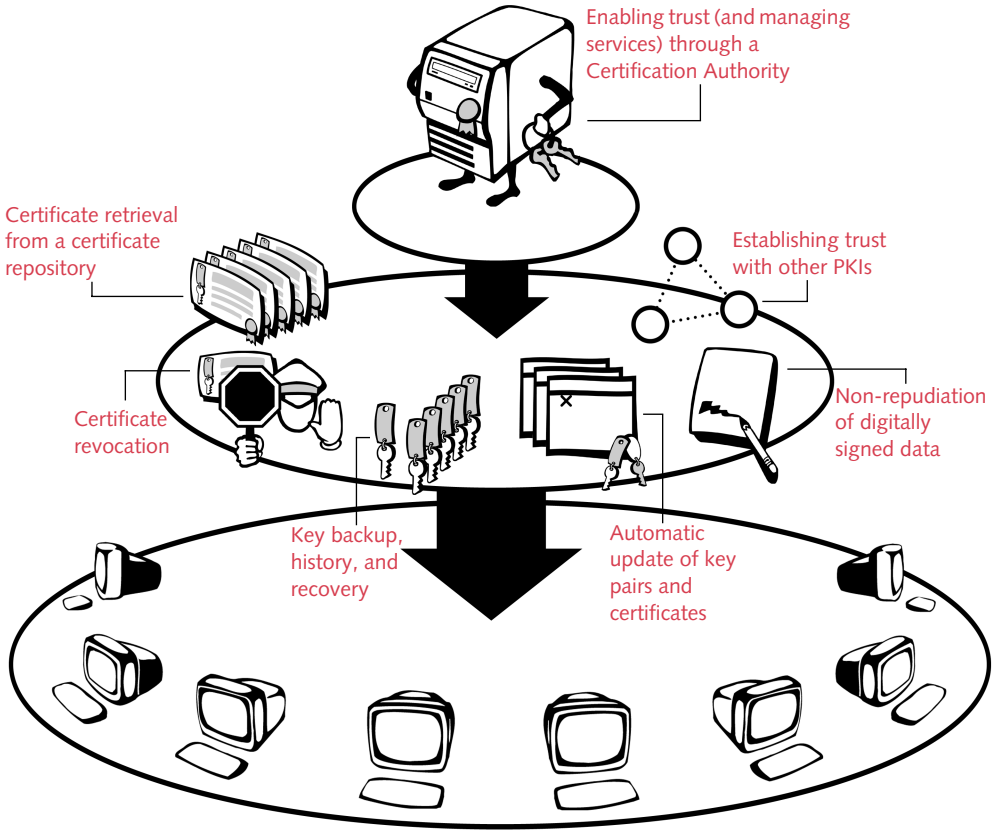
To organize public-key cryptography, certificates, and a Certification Authority in a manner that gives you a manageable, flexible, and reliable form of security, you use a security management system known as a *public-key infrastructure*.

Public-key infrastructure

A public-key infrastructure (PKI) is a framework that provides security services to an organization using public-key cryptography. These services are generally implemented across a networked environment, work in conjunction with client-side software, and can be customized by the organization implementing them. An added bonus is that all security services are provided transparently—users do not need to know about public keys, private keys, certificates, or Certification Authorities in order to take advantage of the services provided by a PKI.

In addition to providing integrity of digitally signed data and protection of encrypted data, a fully functional PKI must provide a number of core services. These are outlined in Figure 1.

Figure 1: Services implemented by a public-key infrastructure



All the above services are supported by client software, ensuring that users participate in a usable, consistent, and transparent PKI.

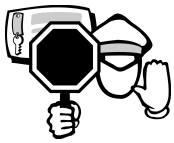
The following sections discuss the core services of a PKI.

Enabling trust through a Certification Authority

The Certification Authority manages the PKI and enables trust among its users. It enables this trust by certifying that the association between a user and their key pairs is valid.

Certificate retrieval from a certificate repository

The PKI's users must be able to locate public keys contained within certificates in order to secure information for other users. They can do this by going to a publicly accessible storage area where certificates can be found, known as a certificate repository.

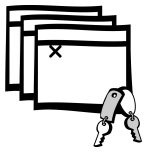


Certificate revocation

The PKI's users must be sure that a certificate is still trustworthy at the time of use. If a certificate is no longer trustworthy, it must be revoked by the Certification Authority. Certificate revocation mechanisms ensure that information about certificates revoked by the Certification Authority is published in a publicly available list (known as a certificate revocation list, or CRL). If a user attempts to use a revoked certificate, they will be informed that use of the certificate is no longer considered secure.

Key backup, history, and recovery

The PKI's users must be sure that they will be able to view data that was encrypted for them, even in cases where they may lose their profiles or forget their passwords. To protect users' access to this data, PKIs perform key backup, history, and recovery tasks for users.

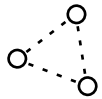


Automatic update of key pairs and certificates

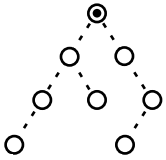
To ensure security, key pairs and certificates must have a finite lifetime. To spare the user the annoyance of having to manually update this information when their key pairs and certificates expire, a PKI can perform this task automatically. Automatic updating keeps things simple for the user, as keys are generated and replaced automatically before they are due to expire. At the same time, security is increased through finite key lifetimes.

Establishing trust with other PKIs

Sometimes users in a PKI community must exchange sensitive communications with users in other PKI communities. For example, two trading partners, each with their own Certification Authority, may want to validate certificates issued by the other partner's Certification Authority. Two ways of creating extended third-party trust among users of different PKIs include



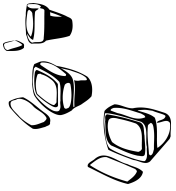
- Peer-to-peer trust—trust is created through two or more Certification Authorities securely exchanging their verification public keys, which are used to verify each Certification Authority's signature on certificates. By signing each other's verification public key, each Certification Authority creates a certificate for the other Certification Authority—thus allowing their users to trust the other Certification Authority. This creates a "peer-to-peer" level of trust among the various cross-certified Certification Authorities.



- Hierarchical trust—trust is created through establishing a "root of trust" among Certification Authorities. Hierarchical trust of Certification Authorities (also known as a strict hierarchy) is a way of arranging two or more Certification Authorities in a restrictive trust relationship. A Certification Authority that's in a hierarchy has its Certification Authority certificate signed by its direct superior. A superior may be the root of a hierarchy, or some level of subordinate beneath the root. The pattern of superiors signing their subordinates' certificates eventually converges at the root, which signs its own Certification Authority certificate. Each subordinate is at the end of a certificate chain that begins with the root's certificate. In effect, all Certification Authorities and users in a hierarchy can trust each other, because they all share a trust anchor (at the root of the hierarchy).

Non-repudiation of digitally signed data

Non-repudiation means that an individual cannot successfully deny involvement in a legitimately signed transaction. To achieve this within a PKI, the key used to create digital signatures (the signing private key) must be generated and securely stored in a manner under the sole control of the user at all times. Since the signing private key is never backed up, or made available to anyone but the user, it is impossible for a user to repudiate data that contains their digital signature.



Client software

Client software is used to support all of the elements of a PKI discussed above. Running from the user's desktop, client software makes trust decisions (for example, whether to use a particular encryption public key contained within a particular certificate to encrypt data) based on signed information that is provided by the PKI. Client software provides security services consistently and transparently across applications on the desktop.

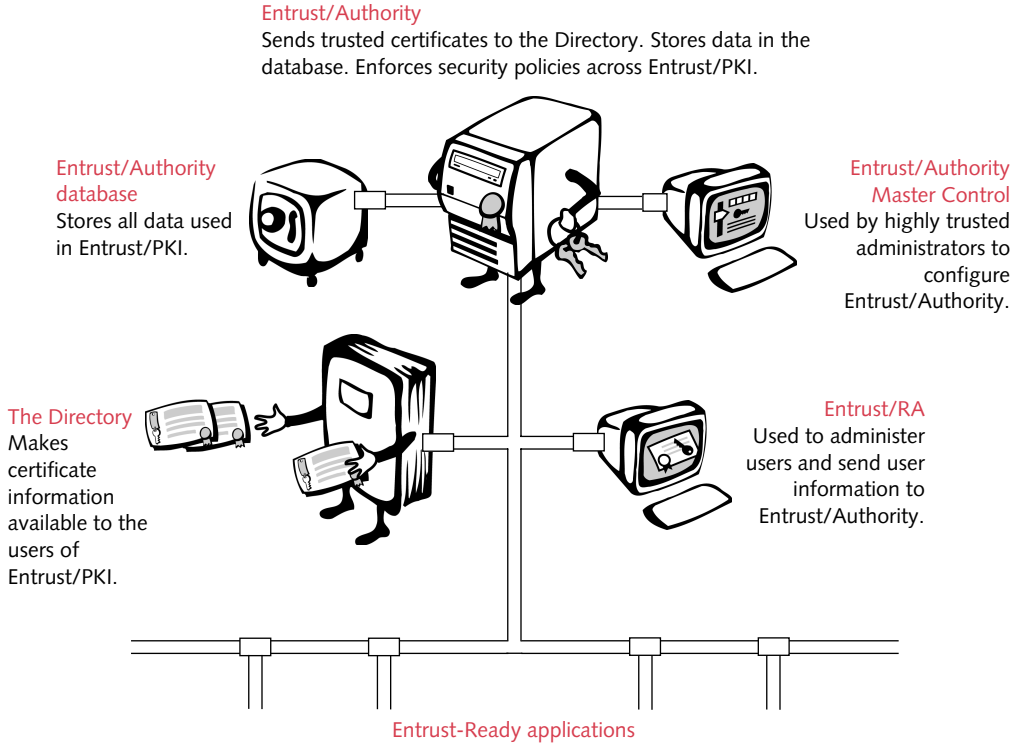
What's Entrust/PKI?

Entrust/PKI is a PKI containing all the features outlined in the section above and more. There is no one, single application called Entrust/PKI—rather, Entrust/PKI is a collection of applications that work together to make up a PKI. The core components of Entrust/PKI are

- Entrust/Authority
- Entrust/Authority Master Control
- Entrust/RA
- the Entrust/Authority database
- the Directory

Figure 2 provides an overview of the relationships among these core components of Entrust/PKI.

Figure 2: Entrust/PKI core components and their relationships



The following sections discuss the core components of Entrust/PKI.

Entrust/Authority

In Entrust/PKI, the role of Certification Authority is held by Entrust/Authority. Entrust/Authority can be thought of as the "engine" of Entrust/PKI. The main functions of Entrust/Authority are to

- create certificates for all public keys
- create encryption key pairs for users
- manage a secure database of Entrust/PKI information that allows the recovery of users' encryption key pairs (in case a user forgets their password, for example)
- enforce the security policies defined by your organization

Access to Entrust/Authority is provided through Entrust/Authority Master Control and Entrust/RA.

Entrust/Authority Master Control

Entrust/Authority Master Control is a local interface with direct access into Entrust/Authority. It provides access to Entrust/Authority to only the most highly trusted administrators (for information on users who administer Entrust/PKI, see "Managing Entrust/PKI" on page 29). Running in either command-line or GUI form, Entrust/Authority Master Control is used for tasks that include

- starting and stopping the Entrust/Authority service
- recovering profiles for Security Officers (for information on Security Officers, see "Security Officer" on page 30)
- managing the Entrust/Authority database

Entrust/RA

Entrust/RA (RA stands for "registration authority") is the administrative component of Entrust/PKI. Entrust/RA uses a graphical interface and communicates securely with Entrust/Authority. Entrust/RA is used for administrative tasks that include

- adding users
- managing users and their certificates
- managing security policies
- cross-certifying with other Certification Authorities
- setting up hierarchies of Certification Authorities

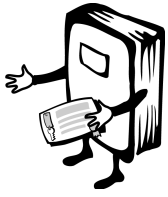
The Entrust/Authority database

The Entrust/Authority database is under the control of Entrust/Authority and acts as a secure storage area for all information related to Entrust/PKI. In this database Entrust/Authority stores

- the Certification Authority signing key pair (this key pair may be created and stored on a separate hardware device rather than the database)
- user status information
- the encryption key pair history (including all decryption private keys and encryption public key certificates) for each user
- the verification public key history (including all verification public key certificates) for each user
- the validity periods for signing key pairs, encryption key pairs, and system cross-certificates
- Security Officer and Administrator information (for more details on users who administer Entrust/PKI, see "Managing Entrust/PKI" on page 29)
- Certification Authority policy information
- revocation information

Note: All information stored in the Entrust/Authority database is protected against tampering, with all sensitive information being encrypted.

Entrust/PKI 6.0 provides enhanced database security with the addition of hardware-based database protection. Hardware-based database protection works by storing a database key on a secured hardware device.



The Directory

The majority of user requests for information involve retrieving other users' certificates. To make this information publicly available, Entrust/PKI uses a public repository known as a Directory. Information that is made public through the Directory includes

- user certificates
- lists of revoked certificates
- client policy information

Note: For information requests and network traffic across Entrust/PKI, the Directory is the most frequently accessed component.

Expanding Entrust/PKI

Working with the core components of Entrust/PKI are numerous Entrust-Ready applications, grouped into four Entrust Solutions families:

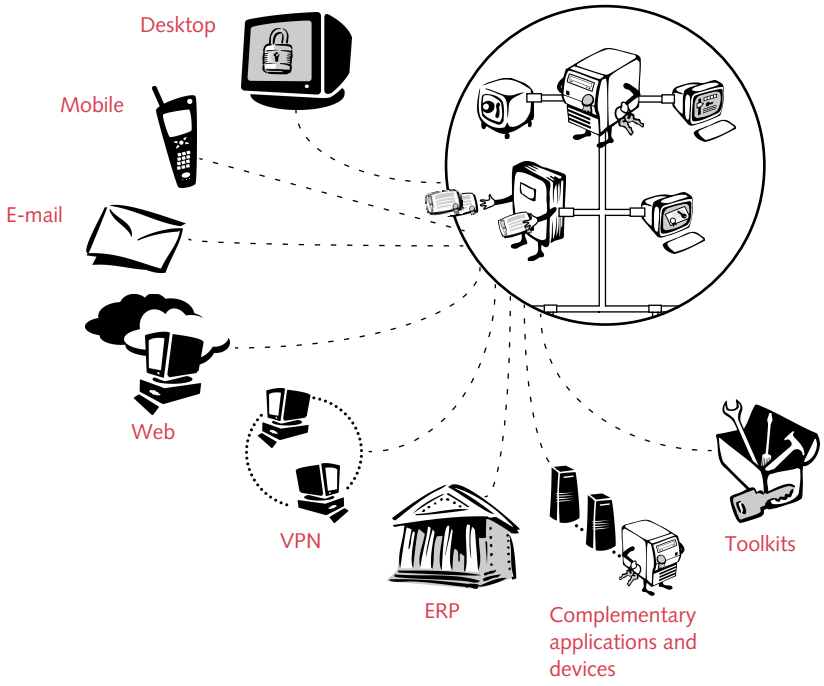
- Enterprise Solutions—including secure file and folder protection, secure e-mail, secure intranet, and secure business processes. All of these decrease the time and expense of internal transactions. Because they bring trust to key processes, they speed such things as electronic workflow, enterprise resource planning, and development of specific applications through toolkits.
- Web Portal Solutions—including authorization, privacy, and digital signatures. These solutions provide trust for online relationships, enabling high-value and sensitive transactions that need persistent legal confirmation. Timestamping provides notarization for further auditing. Built on the integration of Entrust's PKI and authorization solutions, all capabilities will have no footprint and will allow roaming.
- VPN Solutions—including remote office and remote user solutions. These solutions aid the collaboration of a distributed, mobile workforce. They also reduce the costs of inter-office connectivity, compared to leased lines, and reduce operational costs of shared-secret implementations. Entrust has the widest support of VPN solutions.
- Mobile Solutions—including single sign-on, authentication, and digital signatures. These solutions support business over alternative Internet devices. These solutions also enable high-value and sensitive transactions that need persistent legal confirmation. Persistent confirmation is provided by digital signatures. Cable modems are supported in these solutions.

These solutions use Entrust-Ready applications that add increased functionality to Entrust/PKI, provide a greater degree of customization, and add to the number of security services.

These applications are grouped into the following categories, as shown in Figure 3:

- desktop
- mobile
- e-mail
- Web
- virtual private network (VPN)
- enterprise resource planning (ERP)
- complementary applications and devices
- Toolkits

Figure 3: Expanding Entrust/PKI



The following sections provide an overview of some of the applications which work with Entrust/PKI.

Desktop

Entrust desktop solutions provide strong and flexible protection of sensitive data stored on the user's computer desktop. Desktop solutions include five main products: Entrust/Entelligence, Entrust/ICE, Entrust/TrueDelete, and Entrust/SignOn.

Entrust/Entelligence

Entrust/Entelligence provides a common, single layer of security that allows users to log in once to all other Entrust applications (if their policy is set up to allow it). Entrust/Entelligence transparently and automatically manages certificates, encryption, digital signatures, and other security issues on behalf of the user. In addition to these management functions, Entrust/Entelligence can encrypt, decrypt, sign, and verify files.

Entrust/ICE

Entrust/ICE protects sensitive information seamlessly and automatically on workstations, laptops, and network drives by encrypting files in folders.

Entrust/TrueDelete

Entrust/TrueDelete is a utility designed to securely scrub deleted files from the user's system.

Entrust/SignOn

Entrust/SignOn allows users the option to log in once using Entrust credentials to their Windows 95, 98, NT, or 2000 operating system and all Entrust-Ready applications. Entrust/SignOn integrates into Entrust/Entelligence.

Mobile

Entrust Mobile solutions extend Entrust's services and software to support both wired and wireless users accessing the Web portal via alternative Internet devices such as mobile phones and personal digital assistants (PDAs). Mobile solutions include four products: getAccess Mobile Server, Entrust/m-Register, Entrust/m-Validator, and Entrust/DeviceConnector.

getAccess Mobile Server

The getAccess Mobile Server product extends the authentication, fine-grained authorization, single sign-on, and personalization functions of getAccess for a common secure portal for both wireless and wired Web access.

Entrust/m-Register

Entrust/m-Register is a new Entrust product that provides end users with a way to acquire digital certificates over the air, to be used for trusted mobile transactions.

Entrust/m-Validator

Entrust/m-Validator is a new Entrust product that enables the validation of digital certificates used during mobile transactions, through authentication and digital signatures.

Entrust/DeviceConnector

Entrust/DeviceConnector works with Entrust/PKI to issue certificates to devices like smart cards and Hardware Security Modules (HSMs). It address the needs of mobile operators by issuing WAP certificates. Entrust/DeviceConnector can manage these certificates as well as issue them.

E-mail

Entrust/Express provides encryption, decryption, and digital signature capabilities for a wide variety of popular e-mail programs.

Entrust/Express

Entrust/Express is a fully featured e-mail plug-in providing e-mail encryption and digital signature services. It integrates into Microsoft Outlook, Microsoft Exchange, Lotus Notes, and Qualcomm Eudora.

Web

Entrust Web solutions provide a range of offerings which allow users to verify identities, control access to resources, and communicate securely over the Internet. These products include Entrust/TruePass, Entrust/Direct, Entrust/Unity, Entrust/WebConnector, Entrust/getAccess, and Entrust/DeviceConnector.

Entrust/TruePass

Entrust/TruePass is a business-to-business and business-to-consumer solution that enables trusted Web-based relationships. This application provides a provable record of transactions, data protection, and privacy capabilities for online businesses, customers, suppliers, and partners. Entrust/TruePass features a "zero-footprint" client that allows greater user transparency and ease of deployment.

Entrust/Direct

Entrust/Direct is an intranet Web application that allows organizations to deploy e-commerce services on the Web, while providing secure permanent records of user transactions.

Entrust/Unity

Entrust/Unity enables highly interoperable SSL client authorization with standard Web browsers, without digital signatures.

Entrust/WebConnector

Entrust/WebConnector allows unmanaged Web certificates to be issued to standard, off-the-shelf Web browsers and Web servers, thus enabling secure e-business for both vendors and consumers. These unmanaged certificates are not renewed automatically. Entrust/WebConnector can also be used to issue unmanaged certificates to individual Windows 2000 machines for applications such as the Windows 2000 IPSec Client, which is a virtual private network (VPN) client in Windows 2000.

Entrust/getAccess

Entrust/getAccess is an e-business Web portal management solution. It turns a Web portal into a facility for managing relationships with individuals who interact with your organization, allowing you to tailor each user's entire online experience. Entrust/getAccess provides direct access to enterprise applications, while protecting the privacy of individual business relationships and the security of your information assets.

Entrust/DeviceConnector

Entrust/DeviceConnector works with Entrust/PKI to issue certificates to devices like smart cards and Hardware Security Modules (HSMs). It addresses the needs of mobile operators to issue WAP certificates. Entrust/DeviceConnector can manage these certificates as well as issue them.

VPN

Virtual private network (VPN) technology provides network-level security for a wide range of applications. Entrust's VPN solution is Entrust/VPNConnector.

Entrust/VPNConnector

Entrust/VPNConnector provides digital certificates to VPN devices such as routers, gateways, firewalls, and remote access devices.

ERP

Enterprise resource planning (ERP) integrates all facets of a business, including planning, manufacturing, sales, and marketing. Security of ERP applications ensures a reduced risk of loss of revenue, sensitive intelligence, and credibility, while also increasing efficiency, decreasing costs, and expanding business through secured transactions. ERP solutions include Entrust Security for SAP R/3 and Entrust Security for PeopleSoft.

Entrust Security for SAP R/3

Entrust Security for SAP R/3 ensures encryption of data traveling over public networks and provides digital signatures to authenticate both data and messages exchanged and stored within SAP R/3.

Entrust Security for PeopleSoft

Entrust Security for PeopleSoft provides security for PeopleSoft's Win32 and Java clients by replacing password transmission with authentication using managed digital certificates.

Complementary applications and devices

Entrust/PKI's flexibility can be complemented in areas such as administration, notarization, user mobility, and hardware-based security. The applications and devices providing these solutions include Entrust/Roaming Server, Entrust/AutoRA, Entrust/DeviceConnector, Entrust/Timestamp, and Entrust-Ready cryptographic hardware devices.

Entrust/Roaming Server

Entrust/Roaming Server enables a secure, central store of user profiles so that users can log in from anywhere on their organization's network.

Entrust/AutoRA

Entrust/AutoRA provides a secure way to enroll Entrust/PKI users without the involvement of an administrator. Using a Web page tailored for your organization, users can enroll at any time, and from any location. Users can be authenticated with a variety of methods, including use of existing back-end databases.

Entrust/DeviceConnector

Entrust/DeviceConnector works with Entrust/PKI to issue certificates to devices like smart cards and Hardware Security Modules (HSMs). It addresses the needs of mobile operators to issue WAP certificates and of financial institutions that issue certificates to payment cards and Identrus. Entrust/DeviceConnector is not limited to these solutions. It allows the issuance of any certificate supported by Entrust/PKI to devices through a Card Management System. Entrust/DeviceConnector can manage these certificates through the same interface that issues them. This includes management functions like revocation, suspension, and resumption.

Entrust/Timestamp

Entrust/Timestamp provides secure, trustworthy timestamping services to Entrust/PKI users.

Entrust-Ready cryptographic hardware devices

Entrust Technologies offers support for an array of devices that offer tamper-resistant protection to Certification Authority keys and user profiles.

Toolkits

The Entrust/Toolkit Application Program Interface (API) is a family of APIs that provides software developers with low-level access to Entrust Technologies' encryption, digital signature, and automated key management tools. Entrust Technologies' Toolkits enable developers to make their applications Entrust-Ready. The Toolkits provided are

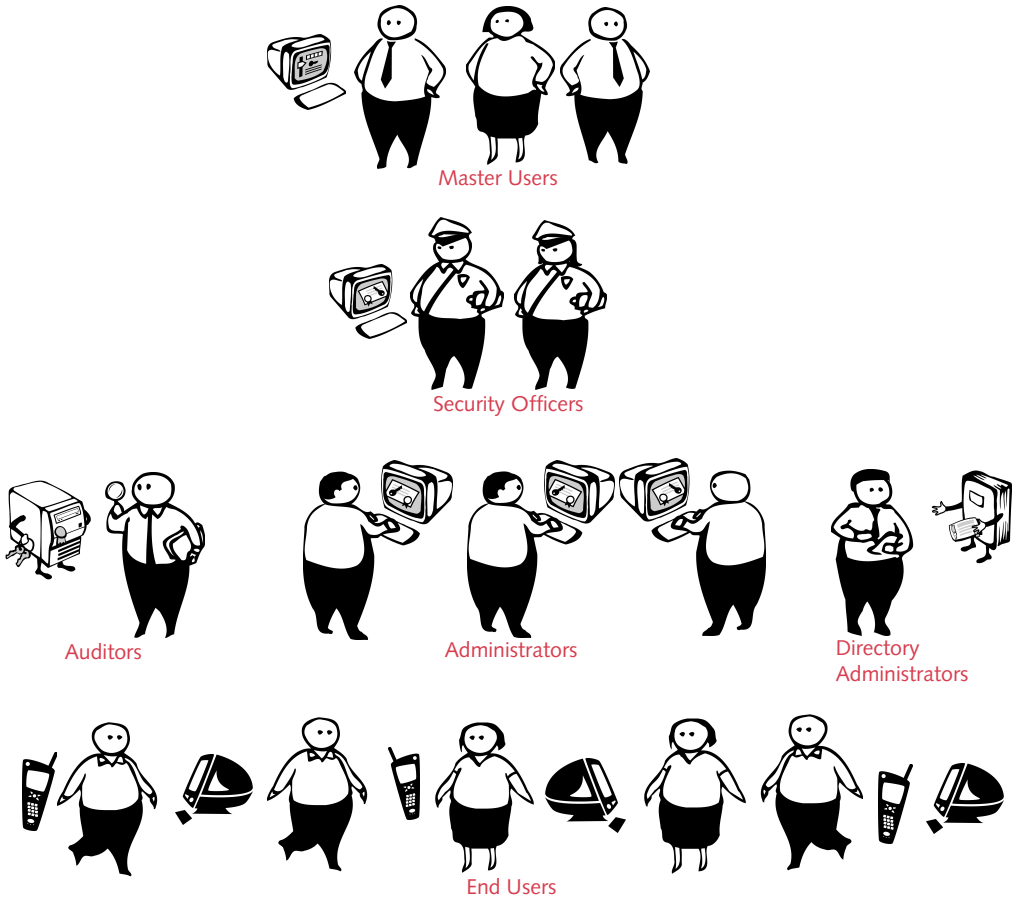
- EntrustFile Toolkit
- EntrustSession Toolkit
- EntrustIPSec Negotiator Toolkit
- Entrust/Toolkit for Java
- Entrust/Toolkit for Visual Basic
- Entrust/Toolkit for SSL/TLS
- Entrust/RA Toolkit

Note: Evaluation copies of Entrust/Toolkit products are available from **http://developer.entrust.com**.

Managing Entrust/PKI

Entrust/PKI provides a division of responsibilities to ensure security, as shown in Figure 4. Supporting this division are a variety of distinct user roles, capable of carrying out the full range of tasks within Entrust/PKI. The default administrator roles in Entrust/PKI are Master User, Security Officer, Administrator, Directory Administrator, and Auditor. The default non-administrator role is End User.

Figure 4: User roles in Entrust/PKI



It is possible to create new administrator and end-user roles and to customize their capabilities. For example, you can create an administrator role that can only carry out certain functions, such as creating users or revoking users. As another

example, you can create several end-user roles, each specifying different key lifetimes for various types of users.

The following sections describe each of the Entrust/PKI default user roles.

Master User

This role is for three highly trusted people who, along with a Security Officer, install and configure Entrust/PKI. Master Users are the only users who can use Entrust/Authority Master Control. Master Users perform system-level operations involving Entrust/Authority, including starting and stopping the Entrust/Authority service.

Documentation used by Master Users consists of

- *Installing Entrust/PKI 6.0 on Windows* or *Installing Entrust/PKI 6.0 on UNIX with Informix*
- *Administering Entrust/PKI 6.0 on Windows* or *Administering Entrust/PKI 6.0 on UNIX*
- *Using Entrust/PKI 6.0 on Windows* or *Using Entrust/PKI 6.0 on UNIX*
- *Entrust/PKI 6.0 and Oracle8i on Solaris*

Note: Unlike other default roles, you can't modify the Master User role or use it as a basis for creating custom roles.

Security Officer

This role is for a few highly trusted people in your organization who will use Entrust/RA to administer sensitive Entrust/PKI operations. The first Security Officer is created when you initialize Entrust/PKI. Security Officers set the security policy for your organization's PKI, and supervise administrators.

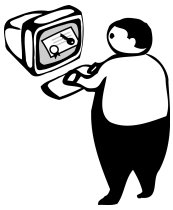
Security Officers use Entrust/RA to perform tasks such as

- setting up Entrust/PKI so that its operations conform to your organization's policies and procedures regarding security
- administering other administrators
- establishing trust relationships with other Certification Authorities

Documentation used by Security Officers consists of

- *Administering Entrust/PKI 6.0 on Windows* or *Administering Entrust/PKI 6.0 on UNIX*
- *Using Entrust/PKI 6.0 on Windows* or *Using Entrust/PKI 6.0 on UNIX*

You can modify this role by changing its name, the number of authorizations required for sensitive operations, and its user policy certificate. This role can be used as a basis for creating a custom role.



Administrator

This role is for any number of trusted people in your organization. For convenience, and depending on the size and nature of your user community, you may wish to have several Administrators. Administrators primarily administer End Users.

Administrators use Entrust/RA to perform tasks such as

- adding, removing, and deactivating End Users
- revoking End User certificates
- recovering End Users

Documentation used by Administrators consists of

- *Administering Entrust/PKI 6.0 on Windows* or *Administering Entrust/PKI 6.0 on UNIX*
- *Using Entrust/PKI 6.0 on Windows* or *Using Entrust/PKI 6.0 on UNIX*

You can modify this role by changing its name, the number of authorizations required for sensitive operations, and its user policy certificate. This role can also be used as a basis for creating a custom role.

Directory Administrator

This role is for any number of trusted people in your organization. Directory Administrators perform tasks that modify information listed in Entrust/PKI's Directory.

Directory Administrators use the Directory Browser tool in Entrust/RA to perform tasks such as

- adding and deleting entries in the Directory, either in batch mode or one at a time
- adding, changing, and deleting attributes in Directory entries

Documentation used by Directory Administrators consists of *Administering Entrust/PKI 6.0 on Windows* or *Administering Entrust/PKI 6.0 on UNIX.*

You can modify this role by changing its name, the number of authorizations required for sensitive operations, and its user policy certificate. This role can also be used as a basis for creating a custom role.

Auditor

This role is for any number of trusted people in your organization. Auditors have a view-only role in Entrust/RA: they can view (but not modify) audit logs, reports, security policies, and user properties.

Documentation used by Auditors consists of

- *Administering Entrust/PKI 6.0 on Windows* or *Administering Entrust/PKI 6.0 on UNIX*
- *Using Entrust/PKI 6.0 on Windows* or *Using Entrust/PKI 6.0 on UNIX*

You can modify this role by changing its name, the number of authorizations required for operations, and its user policy certificate. This role can also be used as a basis for creating a custom role.

End User

This role is for non-administrative Entrust users. End Users cannot log in to Entrust/RA. End Users can be either people (members of your organization) or things (a Web site, a wireless device)—the qualification being that they must be granted a certificate for use within your PKI.

Documentation used by End Users consists of user guides and online help provided with the Entrust-Ready applications they are using.

You can modify this role by changing its name and user policy certificate. This role can also be used as a basis for creating a custom role.

On the client side, the person's name and keys are encrypted, and stored as a profile. The Entrust profile authenticates the users' identities to the Certification Authority and allows them to access their private data. Note that roaming end users do not need to carry their profiles. You can create roaming users if your organization has Entrust/Roaming Server.

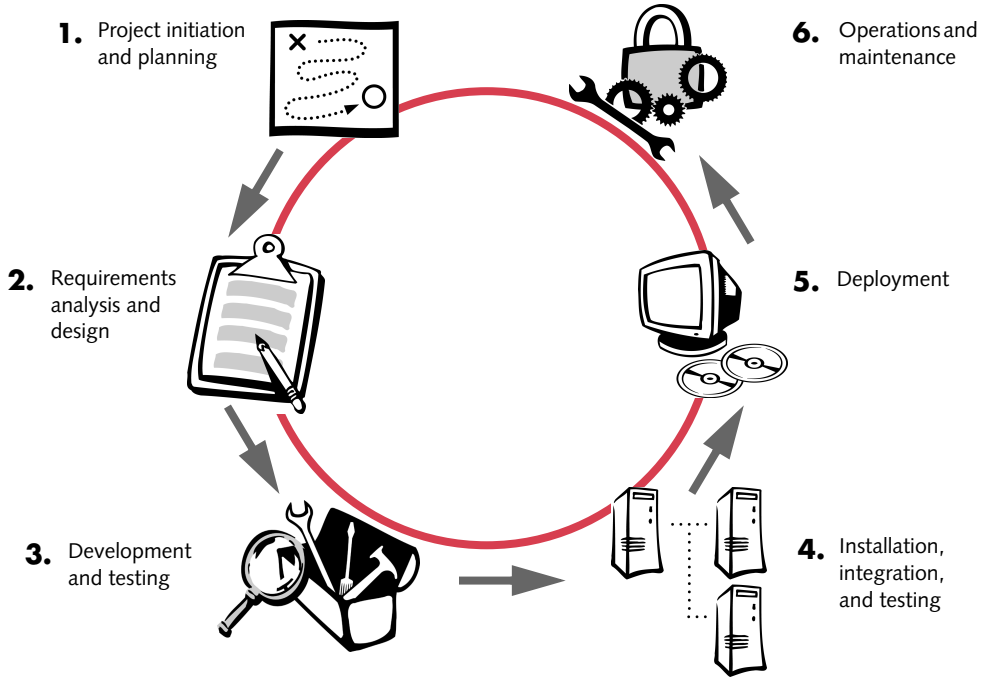
Deployment issues and considerations

Setting up a PKI that suits your security goals involves making numerous decisions before installing any software. To assist your organization in this decision making, Entrust Technologies offers a step-by-step approach to deployment known as the "Entrust Deployment Methodology". The Entrust Deployment Methodology guides organizations in successfully planning and implementing their Entrust security solution.

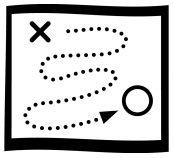
Entrust Professional Services also offers a suite of services that support this deployment methodology. These services provide PKI planning and implementation to organizations who want to jump-start their Entrust security solution.

Figure 5 provides an overview of the Entrust Deployment Methodology.

Figure 5: Entrust Deployment Methodology



The main phases are outlined below.



Project initiation and planning

Project initiation and planning focuses on preparing for your organization's deployment of Entrust/PKI. Project planning involves

- determining and documenting business and PKI requirements
- engaging sponsors and champions within your organization
- engaging functional specialists within your organization
- scoping an initial project
- developing and documenting a project management plan

Requirements analysis and design

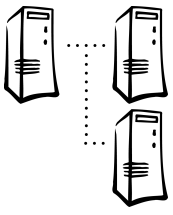
Requirements analysis and design involves assessing what resources, physical or otherwise, are necessary for implementing Entrust/PKI. The focus is on

- analyzing, designing, and documenting Certificate Policies and Certification Practices Statements
- documenting PKI system requirements and design
- documenting PKI facility needs
- identifying staff and training needs
- procuring hardware and software

Development and testing

Development and testing focuses on developing any necessary custom software, as well as testing all software and system components. This takes place before your PKI is installed. Development and testing involves

- developing and testing custom/customized PKI components (if required)
- documenting your organization's PKI operations manual
- enhancing your facilities (if required)
- training PKI operations staff, registration authorities, and help desk staff

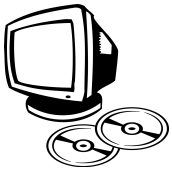


Installation, integration, and testing

In this phase your organization installs all components of the PKI. All operations are closely monitored. Installation, integration, and testing involves

- installing network, firewall, hardware, operating system, and third-party software components
- installing supporting Directory and Web software
- installing Entrust software and supporting hardware

- integrating back-end systems
- testing all functionality



Deployment

Deployment involves running your PKI in a pilot program, followed by full rollout. Deployment consists of

- engaging the pilot user community
- running the pilot for four to six weeks
- monitoring PKI usage and feedback
- monitoring operations staff, registration authorities, help desk staff, and performance
- enhancing the PKI environment as required
- initiating full rollout

Operations and maintenance

With active deployment complete and PKI usage under way, your organization now must ensure continued operation and maintenance. Operations and maintenance involves

- conducting ongoing maintenance and support services
- leveraging the PKI and extending your company's return on investment by deploying additional PKI applications

Other information

The Entrust Deployment Methodology offers other deployment information in addition to the phases listed above. These include

- deployment tips
- provision of best practices
- identification of the project critical path
- identification of the most common critical success factors
- identification of the most common PKI deployment pitfalls
- provision of templates, such as a project GANTT chart

For more details on PKI deployment, Entrust Technologies provides the *Entrust Deployment Methodology Manual*. To obtain this manual, contact Entrust Technologies (see "Advising on PKIs" on page 39 for details).

Where to get assistance

We are always interested in your experiences using Entrust/PKI and its related products and services.

Have comments/suggestions/questions?

We are continually trying to improve the quality and coverage of information related to Entrust/PKI. If you have any comments or questions about any aspect of Entrust/PKI, send us an e-mail at

entrust@entrust.com

You can also visit our Web site at

www.entrust.com

General inquiries can be directed to the following telephone numbers:

- Tel: **1-972-943-7300**
- Fax: **1-972-943-7305**

We look forward to hearing from you.

Telephone, e-mail, and online support

Entrust Technologies offers telephone, e-mail, and online support through the Entrust/Reliance customer care program. Three levels of support are available to meet your needs: Silver Key, Gold Key, and Platinum Key. Information on the three levels of customer support is listed in Table 1.

Table 1: Customer support

Service	Platinum Key	Gold Key	Silver Key
Hours of support:			
• Basic[1]	24x7	24x5 Monday to Friday (EST)	Monday to Friday 8 AM to 8 PM (EST) 7 AM to 7 PM (GMT)
• Emergency[2]	24x7	24x7	24x7
Mutually defined trouble priority	✓	✓	✓
Software maintenance releases	✓	✓	✓

Table 1: Customer support (continued)

Service	Platinum Key	Gold Key	Silver Key
Access to Entrust Xtranet	24x7	24x7	24x7
Early notification of significant technical bulletins	✓	✓	✓
Quarterly service reviews	✓	✓	
Training review	✓	✓	

1. Basic support includes the customer support newsletter, access to online support, and support by telephone or e-mail.
2. Emergency support includes assistance in circumstances where a customer experiences a production system problem (a "production system" is defined as a PKI with active users outside of a test lab environment).

Telephone support

For telephone support, simply call the appropriate number listed in your Customer Resource Kit. The Customer Resource Kit is a package made available to customers after the Entrust/Reliance customer care program has been purchased. You must provide your Unique ID (listed on your Customer Support Xtranet account) whenever you call.

E-mail support

E-mail support is offered to provide assistance for non-critical issues. Questions can be sent to

support@entrust.com

Online support

Online support is provided through the Customer Support Xtranet. This portal contains online versions of product documentation, an information knowledge base, and problem resolutions. It also provides the ability to submit and track service requests via the Web in a secure manner. You must have an account to access this portal. You can sign up for an account at

www.entrust.com/xtranet/support/

Training and certification

Entrust Technologies provides comprehensive training for customers who want to deploy a PKI or implement an e-business portal solution. Our training consists of a combination of theory and hands-on exercises which enables users to quickly maximize their return on investment.

Entrust Courses

Courses offered by Entrust Technologies at the time of the Entrust/PKI 6.0 release are as follows:

- *Entrust/PKI Management* - A hands-on, comprehensive, and detailed look at the components and management of an Entrust/PKI solution.
- *Securing Web-Business Solutions* - A hands-on exploration of the Entrust Web security solutions, highlighting Entrust/TruePass.
- *Hands-on Toolkit Training for Developers* - A comprehensive overview of the Entrust family of Toolkits, with hands-on exercises to give students the experience and skills they need to integrate Entrust into their applications.
- *PKI Policies and Procedures* - An interactive course which gives a detailed look at the Certificate Policies (CP), Certification Practices Statements (CPS), and PKI Disclosure Statement (PDS) documents.
- *Entrust PKI Deployment Planning* - An interactive course which gives a general overview of the Entrust Deployment Methodology, with a detailed treatment of the Entrust-specific aspects of a PKI deployment plan.
- *Introduction to Entrust Desktop Applications CBT* - A self-directed learning tool for end users of Entrust software. It allows them to quickly begin securing files and participating in e-business transactions.
- *Entrust Help Desk Training* - An overview of the basics of security and the architecture and components of the Entrust system. Hands-on exercises give students necessary information to troubleshoot user issues.
- *getAccess Fundamentals and Installation* - A hands-on introduction to the Entrust/getAccess product, providing key concepts, knowledge, skills, and experience necessary to manage Entrust/getAccess.
- *getAccess Customization* - A hands-on course which provides students with knowledge and practice to customize and integrate Entrust/getAccess in their environment.
- *getAccess Boot camp* - Building on previous knowledge of the Entrust/getAccess product architecture and function, this course introduces students to Entrust/getAccess in a distributed environment.
- *getAccess Mobile Server: A Wireless Solution* - A hands-on introduction to the Entrust/getAccess wireless product, its main components, and functions.

For more information about Entrust course offerings or how to register for an Entrust course, please consult

www.entrust.com/training

New courses are constantly being added, so please check the Web site regularly.

Advising on PKIs

In order to operate a PKI that performs to its greatest potential, Entrust Technologies recommends that you consult the Entrust Technologies Professional Services department. Professionals experienced in the areas of PKI planning, implementation, and deployment are available to provide a number of useful services, including

- PKI security consulting
- PKI planning and deployment using the Entrust Deployment Methodology
- systems integration
- an insourcing program

To contact Professional Services about these or other offerings (such as obtaining the *Entrust Deployment Methodology Manual*), please call Entrust Technologies at

1-888-690-2424

Services

Entrust Technologies offers a number of services to meet the ever-growing range of security needs. Two of these services are Entrust.net and Entrust@YourService.

Entrust.net

Entrust.net provides services for issuing and managing digital certificates for publicly trusted Web and Wireless Application Protocol (WAP) servers. These certificates enable secure communications over wired and wireless networks using the Secure Sockets Layer (SSL) and Wireless Transport Layer Security (WTLS) protocols. Certificates issued by Entrust.net are trusted by the vast majority of browsers and wireless micro-browsers in use today. Entrust.net also provides digital signature solutions. For more information, please visit the Entrust.net Web site at

www.entrust.net

Entrust@YourService

Entrust@YourService allows you to secure Business-to-Business, Business-to-Consumer, and Enterprise transactions with PKI technology—while

at the same time outsourcing system hosting, management, and operations. This allows you to achieve the high level of security provided by a PKI without deploying an infrastructure within your organization. For more information on outsourcing the setup and operations of a PKI, without giving up your control over it, please visit the Entrust@YourService Web page at

www.entrust.com/yourservice

Further information on PKI

There are a broad range of sources of information available on PKI technology. A good place to start is by referring to our whitepapers, which can be found at Entrust Technologies' online Resource Center at

www.entrust.com/resourcecenter

For a more comprehensive explanation of PKI, Entrust Technologies recommends the following book:

Understanding Public-Key Infrastructure—Concepts, Standards, and Deployment Considerations

Co-authored by Entrust Technologies' Carlisle Adams and Steve Lloyd, this book provides a thorough examination of the details surrounding PKI. This book will benefit those responsible for planning, deploying, or operating a PKI, as well as serving as an educational tool and reference guide for both novices and professionals alike.

Index

G

T

U

V

W